

Testimony on Unsolicited Commercial Email Comments by David P. McClure, President US Internet Industry Association April 26, 2001

Chairman Burns, and Members of the Communications Subcommittee,

It is my great honor to be invited to testify before you on the subject of Unsolicited Commercial Electronic Mail, and to express the support of our members for S.630, the "CAN-Spam Act." I am particularly pleased to note that this legislation is the product of two of the most respected technology legislators in the United States today, Senator Conrad Burns and Senator Ron Wyden. Our work with these distinguished members of the Senate on other issues has always resulted in the creation of well crafted and effective Internet legislation.

My name is David McClure, and I am President of the US Internet Industry Association, the oldest and largest trade association representing stakeholders in the Internet industry. USIIA was founded by leading companies in the online services industry to represent the interests of individuals and companies that do business on the Internet.

Our diversified membership includes Internet service providers from global and national ISPs to small providers serving remote areas nationwide; Internet backbone companies, telephone companies; hardware and software vendors involved in the technologies of the Internet; electronic commerce sites, and service providers to those sites. Our charter is to promote the growth of electronic commerce, content and connectivity through sound public policy and business support.

The issue of SPAM

For the past three years, much of our effort in public policy has focused on the issue of unsolicited commercial electronic mail. In a white paper authored by Jim Butler and Andrew Flake, we outlined the problems encountered in efforts to stop Spam with a legislative solution, and the scope of legislation that we believe will help bring relief.

I do not need to tell you how serious the problem of Spam is today. According to a report by the Congressional Management Foundation, the Congress itself suffered from more than 80 million pieces of electronic mail last year, the majority of those being unsolicited bulk mailings that interfered with the

operations of Congressional offices and caused real damage to the communications capabilities of this body.

A Gartner survey released last week found that on average an employee spends 49 minutes of each work day simply managing email. That is ten percent of the workday for every employee in every office in America.

In spite of this, and in spite of our personal experiences, and the outcry from consumers and their advocates here today, efforts to legislation against unsolicited commercial email suffer from two problems.

- 1. There is nothing illegal about sending UCE, and it may in fact be largely protected by the First Amendment; and
- 2. We don't know exactly what the term "unsolicited commercial email" means. Certainly, we think we know what "email" is though advancing technology may render even our belief obsolete. I can assure you that we are unable to determine exactly what "commercial" should mean in this context, or "unsolicited," either.

Does it mean that girl scouts who send notices to their neighbors at cookie time should face jail time? Should the American Red Cross be punished for soliciting emergency donations of O-positive blood? We in this room would all agree that these are not the intent of the law. We, after all, only wish to stop the "bad spam."

But I can assure this committee that even in the absence of such laws, anti-spam efforts are abused every day, causing irreparable damage to legitimate businesses. These include trade associations whose newsletters to their own members are routinely blocked by Spam filters. They include one of our member companies that gives more than one million consumers advance warning of viruses and security threats – but find themselves open to liability suits because those warnings are blocked in the name of preventing Spam.

Self-appointed spam blacklisters do not even wait until Spam is sent – they will blacklist your domain, and all of its customers, if they believe that at some future point your service might possibly be used to send Spam. It is vigilante law at its worst.

Solutions

What then, can this committee do?

Must we abandon all efforts to stop unsolicited commercial email in order to protect the First Amendment? Or must we accept the inefficiency and abuses inherent in efforts to stop any message that any person doesn't wish to read? In short, do we see efforts at a legislative solution fail, as they have for the past three years, because we cannot agree on a solution?

No.

In our white paper of three years ago, our association outlined the steps that would provide legislative relief without stumbling over the legitimate rights of communicators or corporations. There are four steps that I would re-state today:

- Let the marketplace do its job. The greatest problem with UCE from an infrastructure standpoint is that it damages the network through its sheer bulk and poor timing. These are both, though, economic issues. Marketers who want to send their messages through an ISP's servers should pay for the privilege. This is a contractual issue that the market is quite capable of managing. And frankly, once email is no longer free and easy to send, its volume will decrease substantially.
- Crack down on fraud. It is estimated that over 90 percent of SPAM today is fraudulent. There is no excuse for this. We should have laws that force mailers to identify themselves, using real email addresses, real header information and real contact information whenever they send a solicitation. Shine the daylight on every commercial message, and woe be to the wicked. Punish the lawbreakers without mercy.
- Support the acceptable -use policies of ISPs. Some ISPs will aggressively filter commercial messages as a service to their subscribers, and those subscribers who desire this service will flock to those ISPs. Others may choose not to block the information, and subscribers will receive what they wish. That is how an open, competitive market works, and the desires of all consumers can be met in this manner.
- Help marketers understand the word, "No." One of the problems with direct marketing is that in spite of the very best and well-intentioned efforts of legitimate marketers, there is always someone who can't understand the word. Opt-out should be simple, pervasive and permanent.

Conclusion

Mr. Chairman, and Members of the Subcommittee, I could ask you to craft the kind of legislation that would cover these four points. But that work is already done. In S.630, we have a very good piece of legislation that will reduce unwanted commercial email and resolve the outstanding legal issues, while still supporting consumer choice and the rights of service providers to run their businesses.

We are here today to ask that you give your support to S.630 as it is today. It does not require re-writing – the industry has had ample time to give input to its authors. It does not require "good faith" exemptions, or private rights of action, or any other major amendment. It needs only your support.

Mr. Chairman, on behalf of USIIA and its members, and of the Internet community at large, thank you for the opportunity to express our views on this issue. I would be honored to answer any questions you might have at this time.

David P. McClure President & CEO US Internet Industry Association 919 18th Street, 10th Floor Washington, DC 20006 (202) 496-9007 info@USIIA.org http://www.usiia.org



The Effective Control of Unsolicited Commercial Email

An Internet Policy White Paper
By

James W. Butler III Andrew Flake

Introduction

As commonly used, the pejorative "spam" refers to bulk electronic mailings of a commercial character, and the practice of "spamming" is positioned squarely at the center of contemporary debate over the Internet's commercial development, Internet etiquette and individual privacy.

For Internet service providers ("ISPs") especially, the bandwidth commandeered by spamming and the resultant slowdowns in service represent an infrastructure expense of increasing dimensions. At the same time, the law of the Internet remains in some disarray, although courts and even some states have taken initial stabs at regulating spam.

This White Paper presents a discussion of the problems inherent in direct electronic marketing from the perspective of both consumers and of the online community and concludes with modest recommendations for salient legislative initiatives.

Historical Overview

Spam is only one of a host of new legal issues that have arisen around electronic mail, and the term itself has had several incarnations in the online and Internet communities.

During the Internet's pre-commercial days, amid the perception of the need to minimize utilization of servers and message traffic to conserve acaUCEic and research resources, "spamming" referred to the act of posting an individual message to numerous UseNet Newsgroups. The exact path by which it did so is not known, but at some point the earlier, rather clean definition of "spam" evolved to encompass commercial or marketing messages as well.

One of the more critical events in the term's migration came with the infamous postings of an attorney who initiated a massive e-mailing in the hopes of soliciting green-card business among immigrants. His multi-posting efforts gained him the permanent enmity

of Internet and Usenet users, as did his unwillingness to cease the effort once informed of his breach of Internet manners, or "Netiquette." That violation occurred simultaneously with explosive growth of Internet use among consumers: as they poured onto the Internet in 1994-1996, the sheer number of new users overwhelmed the online community and made the maintenance of the tightly-integrated Internet culture virtually impossible.

Despite very strong efforts by experienced Internet users to maintain their traditions and definitions, the communication became garbled, and two Internet conventions (one barring messages with commercial content, the other barring multi-posting of messages) were generally commingled into the general heading "spam."

The Terminology of Electronic Messaging

Whatever its traditional definitions and usage, the term "spam" may today be taken or mistakenly referred to as any one of the following sorts of messages: a message with commercial or marketing content; one that the recipient does not wish to receive, or which is unsolicited; one that the recipient has not specifically authorized in advance of its transmission; or, a message posted multiple times to a single or multiple newsgroups.

Accepting the Internet's transition into a commercial entity in which some forms of marketing and sales messages will be accepted and essential, imprecise definitions are counterproductive and serve to limit the development of electronic commerce.

Although it is not the intent of this White Paper to alter Internet culture or common usage of terminology, the confusion and imprecision associated with the word "spam," suggest that a more precise labeling would be beneficial.

This White Paper will use the term Unsolicited Commercial Electronic mail ("UCE") to describe the process of directing a commercial message via electronic mail to a selected group of recipients.

Scope of the Problem

Measured by volume of use, electronic mail is fast approaching more traditional means of communication, including letter-writing and telephone communications. Though abuse of the UseNet messaging system on the Internet is both rampant and detrimental, the current controversy over electronic communication more frequently centers on unsolicited commercial email. UCE is a problem for the Internet, for five reasons:

- It is inefficient. Presently, with no controls or costs attached to UCE, it is as cost-effective to drop one million pieces of UCE onto an ISP as it is to drop one though the costs to the ISP are substantial. No production cost is involved in the creation of e-mail intended for UCE distribution no brochures, artwork, printing or other mechanical costs. In effect, unchecked UCE is a "free ride" for marketers and provides them with a disincentive to research, focus or target the list of recipients to insure interest in the products or services presented.
- It disrupts service. A major mechanical drawback with UCE is that it arrives on the Internet without notice. It slows service for other users, often during peak use hours. In some cases, it has caused wholesale failures of Internet networks. This disruption is frequently aggravated by the fraudulent use of incorrect or nonexistent return addresses, which causes the outraged responses of recipients to bounce across the network multiple times as the system attempts to deliver messages that cannot be delivered.
- It is frequently fraudulent. An Internet culture protective of user anonymity has the unfortunate side effect of creating an environment in which unscrupulous purveyors of UCE can operate. Messages are sent directly to an electronic mailbox, and marketers need not provide information, e.g. business name,

physical address, telephone and fax numbers, that would enable consumers to assess the validity of companies. Without greater certainty about company legitimacy, Internet consumers quite rationally become wary of even legitimate marketers. These concerns have contributed to decisions by ISPs to seek judicial protection.

- There is no effective "opt out" procedure. In the offline world, marketers operate a system that enables consumers to remove themselves from direct marketing lists. While the system is not completely effective, it does exist. In the online world, no such system exists, although numerous efforts to create one have been undertaken.
- There is no compensation for service. In the offline world, direct marketing subsidizes the US Postal Service and/or telephone companies, effectively paying for itself. In the online world, UCE currently benefits only the originator of the message and does not pay for the burdens it places on the system. UCE provides very little value, e.g., convenient shopping, entertainment value, or consumer information, and Internet service providers bear the brunt of the resource outlay for the infrastructure that enables UCE. Realistically, a mechanism that shares the economic burdens of UCE will more closely mirror the offline world, and will produce stronger efficiencies in the way UCE is handled on the networks. A "pay as you go" system would compensate the ISP's who provide the on-and-off ramps for the UCE traffic.

Combating the Growth of UCE

In recent years, significant progress has been made toward understanding and dealing with the problems associated with UCE. Sanford Wallace, self-proclaimed "king" of the UCE business, stepped down and joined the ranks of those opposing unchecked direct

electronic marketing. Major Internet providers such as Earthlink and AOL successfully secured court orders against perpetrators of unwanted UCE. Nonetheless, the current legal situation remains far from clear, and debate rages on among those impacted by and involved with Internet service provision.

On one side are individual consumers who do not wish to have their time wasted by having to open and read the first few lines of countless messages in which they have no interest. ISP customers who fall into this group are supported by consumer advocacy groups, as well as by those whose loyalty to the old Internet culture of non-commercialism eschews marketing of any sort. On the other side are the marketers, who believe that they have a clear right to communicate with current and potential customers, regardless of legal trends to the contrary. These marketers are supported by customers who wish to have product and service information, as well as by the Direct Marketing Association and its legion progeny, who fought for similar rights in the use of the mails and in direct telephone solicitation.

Individual ISPs straddle the line and await some clear resolution while attempting to cope with UCE's associated costs - these are the online and Internet services that suffer both the wear on their systems from dumping of UCE messages, along with the wrath of the subscribers incensed over wasted time and service slow-downs. These service providers seek additional sources of revenue to keep costs competitive as their business grow, but fear the network damage and other consequences of opening their systems to unwanted UCE.

Unsuccessful Initiatives

While the two camps (and the companies and individuals stuck in the middle) have generated significant public dialogue, attempts to deal with the very real and escalating problems of UCE have been only partially successful, and generally only in the event

that the originator of the UCE can be identified. Initiatives that have proven unsuccessful include:

- Attempts to claim ownership of the electronic mailbox. Unlike the offline world, where the US Postal Service rather than the consumer owns the mail box, the online industry assumes that each individual owns his or her email box. Although such ownership has not been legally established, the constitutionality of so-called "receiver restrictions," in which consumers are given the right to refuse certain mailings, has been upheld.
- "Right to privacy" claims. There is a perceived "right" of consumers to not have to view anything they elect not to view, although no case law substantiates this position. By the same token, however, constitutional free speech does not mean that an individual is *obligated* to view particular subject matter.
- Protection Act of 1997," H.R. 1748, 105th Cong., 1st Sess. (1997). Although the laws that were used to prohibit direct marketing via fax automatically are sometimes believed to extend to electronic mail, this concept overlooks some very fundamental differences in the two systems. For one, fax machines use expensive resources, where electronic mail normally does not, and efforts to build a case based on the time wasted in reading unwanted e-mail have largely been countered by advances in message preview technology and the by move to flat-rate rather than per-minute pricing for Internet and online services.
- An "opt-in" solution, no matter how desirable, may be impractical. Much of the discussion of consumer rights to date has focused on whether UCE should be sent only to those who have specifically requested communications -- an "opt-in only" solution. This approach, however, would severely limit communication with persons who have not given advance written consent.

- An "opt-out" solution needs strong enforcement mechanisms. The ability of consumers to quickly and easily "opt out" of receiving UCE, will only work if there is a sufficient incentive to keep the opt-out list well-maintained, well-promoted and easily accessible by consumers.
- Efforts to delineate UCE based on the content of the messages has proven impractical. For example, even the most liberal definitions of "commercial" email would prevent announcement to parents of what an elementary school is serving for lunch, since this would clearly be an advertisement of a product for sale.
- Use of mandatory "header" information is counter-productive. Many suggestions have been made regarding an identifying mark or phrase that could be placed in the subject line or at the head of any commercial message, thus allowing e-mail filters to more easily identify and eliminate UCE. While this idea is appealing, it suffers from the definitional problems because filtering systems, at their current level of sophistication, cannot differentiate between UCE and otherwise valid customer mailings. Attempting to have any body, organization or regulation define exceptions to the rule would be unwieldy, and use of extensive identifying information in the first lines of the message would render useless the preview screen technology used by many consumers to rapidly screen messages and their content.
- Use of a "pre-existing relationship" test may not be sufficient. It has been assumed by many in the online community that such a test may be implemented in the near future, under which electronic mailings would be permitted to those customers and other groups with whom the mailer has a "pre-existing relationship." This assumption, however, has led virtually every business that has a web site or advertises via electronic mail to scramble to collect personal information about users as a hedge to show such a relationship. The rampant collection of data in order to prove the relationship has created another crisis in

the area of privacy, as was noted by the Federal Trade Commission in its efforts to enforce Internet privacy guidelines.

Developing A Framework

To merely legislate or regulate UCE out of existence is neither Constitutional nor necessary. Though not yet tested, even unsolicited commercial messages would be subject to constitutional protections if Congress acted to prohibit their dissemination.

Such restrictions are better left to internet service providers, which as private actors may ban distribution of UCE messages on their networks. Still, the industry's efforts with respect to UCE have so far proved only moderately successful. From these efforts, however, has emerged a sense of a viable framework to address its inherent problems.

- Fraud Prevention Legislation. The extension of regulations and legislation related to fraud to UCE. The trend at the state level is clearly toward regulating the practice of UCE. State legislation, however, must be carefully drafted to avoid constitutional challenge, as the experience of Georgia's UCE fraud statute indicates.
- Measured Common Law Development. Recognition by the courts that UCE as presently practiced creates a strong adverse impact on the Internet. Specifically, the channeling of hundreds of thousands of pieces of electronic mail through an Internet system at a single time significantly degrades the performance of the network and interferes with other forms of Internet access and communications.
- Continued Industry Initiatives. The growth of filtering technology for electronic mail. While still crude and relatively ineffective for the larger body of electronic messages, filtering technology has assisted ISPs in taking the first steps toward empowering consumers to automatically reject unwanted solicitations.

Any proposed framework will at best be preliminary, with additional time and consideration required for its full effectiveness, but reasoning from the current experience of the online industry, it is certain that the following will be factors in any consistent legislative approach to UCE:

- The first step is to eliminate fraudulent mailings. The most critical elements of a framework for control of UCE will be unsuccessful if unscrupulous operators are able to flaunt the rules with impunity. At a minimum, electronic mailers should be required to divulge their real identities and return addresses, as well as compliance with other consumer protections laws as appropriate. Although a number of ISPs have imposed guidelines prohibiting the use of their services for the sending of UCE messages, such efforts are far from universal, and the individual policies of an ISP provide no protection against external sources of UCE.
- The solution must include **relief for stress on the networks**. Consumer irritation aside, the damage done to the Internet by UCE is very real, and its elimination of this damage must be a central consideration in proposed legislation. At the minimum, a requirement for contractual notification of the Internet service or provider prior to transmission of UCE should be put in place; the market would be best served, however, by an industry-wide financial arrangement, similar to the postage system, to compensate all carriers of the message traffic. A compensation system would have the additional benefit of providing a barrier to entry for unscrupulous spammers.
- The right of the states to impose more stringent consumer protections should be preserved. State and local laws have provided some of the strongest protections against abusive UCE to date, in part because they have more extensive protections available against business interference and detrimental business practices. The framework for the future should include some assurance that state and local considerations on behalf of Internet services and consumers

not be preempted, to the extent that they are more solicitous of consumer interests than any federal statutory cause of action. Federal initiatives should provide a base level of protection for consumers and ISPs, to circum vent the possibility of inconsistent regulation of an entity, the Internet, that is not bounded by geography.

Conclusion

The continuing popularity of electronic mail ("e-mail") as a medium of personal and business communication has brought in its wake a host of novel legal issues, among them the extent to which the practice of unsolicited commercial email ("UCE") may be limited.

A compelling need to protect Internet users from unwanted, unnecessary and fraudulent commercial message traffic, as well to protect the infrastructure of the Internet from the problems created by massive postings of messages, either commercial or otherwise, has already seen some courts and state legislatures move to prohibit the practice in its various forms.

This White Paper has set forth in summary fashion the historical and legal underpinnings of the debate over UCE, and its conclusion is that federal legislation should be enacted that would (1) provide a minimum of protection for consumers against fraudulent electronic mailings by marketers; and (2) promote a more reasonable allocation of the costs of legitimate UCE toward the direct marketers that are its source.

Appendix A: USIIA Policies

The US Internet Industry Association opposes any action, program, system or endeavor that corrupts the legitimate use or integrity of the channels of electronic communication. This policy is explicitly stated in paragraph 7 the USIIA Code of Standards, which reads as follows:

"Members shall not knowingly create, acquire, distribute or allow intentional distribution of materials that violate the legitimate use or integrity of the channels of electronic communication, online services, computer systems or their contents."

-- USIIA Code of Standards.

Consistent with this policy, USIIA does not support the practices of Multiposting of Messages or Off-Topic Posting of Messages. It is the believe of the Association that persons who deliberately engage in these practices should have their access to the Usenet and other online lists, discussion groups or message bases terminated. This policy is not intended to affect the legitimate act of Cross-Posting of Messages. Similarly, USIIA does not support or condone the communication of information that is deliberately misleading or fraudulent. This is stated in the USIIA Code:

"Members shall not knowingly disseminate false or misleading information and shall act promptly to correct erroneous communications for which he or she is responsible, or which originated from or resides on his or her system." USIIA Code of Professional Standards, #8.

This section of the Code is interpreted to include messages in which an attempt is made to disguise the commercial nature of the message, those which are fraudulent, those which misrepresent the origination of the sender, and those which are violations of the law at the point of origination. Nothing within the Code, the Bylaws of the Association, its Mission Statement or the will of its members specifically prohibits or discourages the legitimate commercial uses of electronic mail or messaging.